Remarks

This amendment responds to the official action mailed January 11, 2007 and is accompanied by a petition for one month extension under 37 C.F.R. §1.136(a) and the required official fee.

Claims 4, 5, 7, 8 ,18 and 19 were considered indefinite for inclusion of mathematical formulas. The claims have been amended to more particularly and distinctly define the aspects of the invention in narrative form. The aspects now described in a functional narrative are embodied in the original formulas and description, and therefore, no new matter is presented.

The invention concerns a "fair" exchange of hidden values that obscure digital certificates or passwords or the like, by a mathematical function such as exclusive-OR or modular multiplication. There is a risk in exchanging values of this sort that one party might induce the other to reveal a hidden value, but will not in turn reveal his own hidden value. This can put the revealing party at a substantial disadvantage.

According to the invention as disclosed and claimed, sequences of values are revealed and exchanged according to an iterative process wherein each iteration brings the two parties closer to the point at which it is possible for both of them to derive the full hidden information of their respective adverse party. If either party defaults and discontinues the process or does not conform with the process (which conformance is verifiable), then at that point the defaulting party and the non-defaulting other party, by expending additional processing steps, have a comparable ability to derive the complete hidden information of their respective adverse party.

According to the invention, the iterative process of exchanging information comprises establishing a modular function known to the first user and known to the second user. The modular function iteratively produces a plurality of sequence values. Each such sequence value is related, according to the modular function, to the next previous sequence value, whereby conformance to the modular function can be

determined. At the end of the process, the parties each have access to the adverse party's full hidden value. A total number of iterations is established by agreement of the parties; and according to applicant's dependent claims the number is at least eighty.

According to an aspect of the disclosed embodiments, the number of processing steps needed to advance according to said modulus function, between the adjacent ones of said sequence values, increases and decreases symmetrically during the iterations, about one of said sequence values at a known position in the sequence. During the iterations as disclosed and claimed, the first and second users successively disclose values that lead up to end of the sequence. The point is that with knowledge of the modular function and knowledge of the manner of the exchange, each party can verify at every step that their counterpart is going ahead as they committed to do. If either party should renege, neither party is at substantial disadvantage because both parties have a comparable computing job to reach the end of the sequence from the information that they have received up to the point that their counterpart reneged.

If the entire sequence of exchanges is completed, both users obtain their adverse party's hidden data, which (as stated in a dependent claim) can be the second last value in the exchange sequence.

If the exchange is terminated deliberately or otherwise, both parties are comparably close to obtaining the other party's hidden data at that point (if not equally close, at least they are comparably close). The exchange is fair.

According to the invention, the processing "distance" is an extent of computing operations. These can be arranged so that the number of steps needed to advance according to the modular function differs during the iterations. Applicant's disclosure provides an example wherein the sequence from one value to the next involves squaring or exponentiation by different number of times, that number of times being greatest at the middle of the sequence of values and the number being smaller approaching the end. See paragraph [0032] and the example sequence in paragraph [0039].

Each user reveals his/her next sequence values proceeding toward the end of the sequence. It is possible for each user to determine whether their adverse party is in conformance with the rules because the successive high or low end values can be

tested for exponentiation according to the modular function. As the process proceeds, there can be a change in the stepwise computing load (especially the number of exponentiations per step) needed for a receiving party to obtain the next sequence value by continuing to apply the modular function, as opposed to obtaining that next sequence value from the other party.

Such a technique is not found in the prior art. According to the Asokan reference (US pub. 20020049601), a series of values are exchanged. The examiner notes that Asokan does not specifically disclose difference values between adjacent ones of the sequence values are symmetrically distributed about one of said values of a known order. In the official action, it is asserted that Micali (US 4,944,009) discloses a symmetrical distribution of sequence values about one of the values in known order, rendering the invention obvious from a combination of Asokan and Micali. Reconsideration is requested.

Asokan requires invoking sub-protocols and the participation of an impartial party in some circumstances. Such techniques do not disclose or suggest the idea of using sequential exponentiated values in a way that permits both users to approach the ability to discern the adverse party's full hidden information, in steps characterized by varying processing loads to progress between the successive values as the process of exchange is carried out. According to applicant, there is never a need for an impartial arbitrator because applicant's idea is not to decline to disclose a hidden value if the other party has not reciprocated. Instead, an aspect of the invention is that once both parties are committed, they each need to expend a comparable computing distance (a comparable number of exponentiations of modular function values) to reach their counterpart's hidden value from the last disclosed values.

Asokan is combined in the official action with Micali. Micali is cited for providing values that are symmetrically distributed about one value of a known order. Reconsideration is requested. Micali's teaching is simply that of a pseudorandom number generator. It is possible that a pseudorandom number generator might produce a symmetrical distribution of values, but the values are merely a sequence of random numbers without a useful structure or sequence such as found in applicant's invention. There is no teaching or suggestion from Asokan or Micali, or from any routine

combination, that would lead a person of ordinary skill to impose a useful structure or sequence. Asokan and Micali cannot be seen to lead a person of ordinary skill routinely to cause values obtained by computational steps such as exponentiation, to require more or fewer computational steps as the process proceeds toward its end. Micali's random number generator does not teach anything that would help the person of ordinary skill to modify Asokan in a way that might lead toward applicant's invention.

Applicant's values are more than an succession of random values. They are values that adhere to a function (progressively advancing numbers of squarings or exponentiations) that enable the receiving part to test that the values, proceeding upwardly and downwardly from the ends of the list toward the center of symmetry or otherwise up to the end of the sequence, are proceeding according to the agreed function. Applicant's values demonstrate the continuing participation and good faith of both parties to the transaction. The prior art does not approach the matter of fairness of exchange in a comparable way.

The claims have been amended to resolve formal matters, and in particular to state in a narrative way what it is about the formulas that makes applicant's invention novel and unobvious. It is possible that others such as Asokan have sought ways to render an exchange of hidden values fair, but their solution is to ensure up to the final exchange that if one party reneges, that party does not obtain the other party's hidden value. Applicant's invention relies on a different idea, namely to ensure that the goal of obtaining their opponent's hidden value is more or less equally far out of reach for both parties. If one party reneges, even very late in the process, it is not substantially easier or harder for that party to obtain the other party's hidden value, than it is for the other party to obtain the hidden valued of the reneging party.

The claims have been amended to more particularly and distinctly define the invention. The formulas in the claims have been replaced by a narrative of steps and programmed computations. No new matter is presented. The invention claimed as a whole is not shown by the prior art of record. There is no basis to conclude that the Asokan and Micali disclosures could be routinely combined or applied to produce a method or computing system that meets the subject matter claimed as a whole.

The remaining pending claims 1, 3, 4, 6, 7, 9, 10 and 23-25 are believed allowable as now presented. Reconsideration and allowance are requested.

Respectfully submitted,

Date: May 10, 2007

/Stephan Gribok/
Stephan P. Gribok, Reg. No. 29,643
DUANE MORRIS LLP
30 South 17th Street
Philadelphia, PA 19103-4196
tel. (215) 979-1283
fax.(215) 979-1020
SPGRIBOK@DUANEMORRIS.COM

Docket No.: Y0242-294
[Garay 10-1]